Telematics" by Komatsu et al.; and EP Publication No. 0 581 317 A2) that were discussed during the interview of December 4, 2001.

Definitions

Applicant proposes changes to the definition previously set forth in the Interview Summary of December 4, primarily to recite the inclusion of a key, but also to make clear that the seed may be random or pseudo random. In particular, Applicant submits the following definitions to more particularly define terms for use in understanding Applicant's invention (changes from the definition recited in the interview summary are underlined):

A stega-cipher (a.k.a. a steganographic cipher) is an algorithm or combination of algorithms that performs two functions: (1) a steganographic function to determine where in the carrier signal, data (such as message data or watermark data) can be hidden "in plain view"; and (2) a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that randomly maps the message data into the carrier signal. The use of the phrase "in plain view" does not limit the claimed invention to visual applications.

The carrier signal is defined as the digital data that is being protected (such as a video image or audio).

Support for Definitions

Applicant identifies the following portions of the specification as support for the definitions provided above (emphasis being added using underlining):

Specification--Page 7, Lines 10-25:

> The practical considerations of weak encryption schemes and rogue engineers have served to limit the faith which may be put in such copyright protection schemes. The invention disclosed herein serves to address these problems with conventional systems for digital distribution. It provides a way to enforce copyright online. The invention draws on techniques from two fields, cryptography, the art of scrambling messages so that only the intended recipient may read them, and steganography, a term applied to various techniques for obscuring messages so that only the intended parties to a message even know that a message has been sent, thus it is termed herein as a stega-cipher. The stega-cipher is so named because it uses the steganographic technique of hiding a

message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content. The message itself is encrypted which serves to further protect the message, verify the validity of the message, and redistribute the information in a random manner so that anyone attempting to locate the message without the keys cannot rely on pre-supposed knowledge of the message contents as a help in locating it.

Specification, Page 8, lines 7-14:

The invention disclosed herein combines two techniques, steganography--obscuring information that is otherwise in plain sight, and cryptography--scrambling information that must be sent over unsecured means, in a manner such that only the intended recipient may successfully unscramble it. The net effect of this system is to specifically watermark a piece of content so that if it is copied, it is possible to determine who owned the original from which the copies were made, and hence determine responsibility for the copies. It is also a feature of the system to uniquely identify the content to which it is applied.

Specification, Page 8, line26 - Page 8, line 2:

The invention improves upon the prior art by providing a manner for protecting copyright in the digital domain, which neither steganography or cryptography does. It improves specifically on steganography by making use of special keys which dictate exactly where within a larger chunk of content a message is to be hidden, and makes the task of extracting such a message without the proper key the equivalent of looking for a needle in a haystack.

Specification, Page 9, lines 8-14:

The information encoded by the Stega-Cipher process serves as a watermark which identifies individual copies of content legally licensed to specific parties. It is integral with the content. It cannot be removed by omission in a transmission. It does not add any overhead to signal transmission or storage. It does allow the content to be stored to and used with traditional offline analog and digital media, without modification or significant signal degradation. These aspects of the stega-cipher all represent improvements to the art. That is, it forces would-be pirates to damage the content in order to guarantee the disabling of the watermark.

Specification, Page 9, lines 18-20:

The invention uniquely identifies every copy of multimedia content made using the invention, composed of digitized samples whether compressed or

uncompressed, including but not limited to still digital images, digital audio, and digital video.

Specification, Page 10, lines 9-11

It is considered that statistical data spreading and recovery techniques, error coding or spread spectrum processing techniques might be applied in the invention to handle the effects of lossy compression, or counter the effects of a randomization attack.

Specification, Page 12, lines 9-19

The program described in more detail below combines the techniques of cryptography and steganography to hide a securely encrypted digital copyright certificate which contains information satisfying the criteria listed above, in such a manner as to be integral with the content, like a watermark on paper, so that possession of the content dictates possession of the watermark information. In addition, the watermark cannot be "found" or successfully decoded, without possession of the correct "masks" or keys, available only to those legitimately authorized, namely, those parties to a commercial transaction involving the sale of a copy of the content. Finally, the ability to distribute such watermarked content in a system which implements the watermark scheme is denied without a successfully decoded watermark. Because well known and tested cryptographic techniques are used to protect the certificate itself, these certificates are virtually impossible to forge. Finally, the watermark cannot be erased without significantly damaging the content.

Specification, Page 13, line 1-11:

The value of the stega-cipher is that it provides a way to watermark the content in a way that changes it slightly, but does not impact human perception significantly. And, furthermore, that it is made difficult to defeat since one must know exactly where the information resides to extract it for analysis and use in forgery attempts, or to remove it without overly degrading the signal. And, to try to force copyright information one must first be able to analyze the encrypted copyright information, and in order to do that, one must be able to find it, which requires masks.

Specification, Page 16, lines 27-page 17, line 2:

These changes are minimized so as not to adversely affect the perceived quality of the reproduced audio signal, after it has been encoded with additional information in the manner described below. In addition, the location of each of these changes is made virtually impossible to predict, an innovation which distinguishes this scheme from simple steganographic techniques.

Specification, Page 18, line 5 – page 24, line 9 (selected portions produced below):

III. Example Embodiment of Encoding and Decoding

A modification to standard steganographic technique is applied in the frequency domain described above, in order to encode additional information into the audio signal.

In a scheme adapted from cryptographic techniques, 2 keys are used in the actual encode and decode process. For the purposes of this invention the keys are referred to as masks. One mask, the primary, is applied to the frequency axis of FFT results, the other mask is applied to the time axis (this will be called the convolution mask). The number of bits comprising the primary mask are equal to the sample window size in samples (or the number of frequency bands computed by the FFT process), 128 in this discussion. The number of bits in the convolution mask are entirely arbitrary. This implementation will assume a time mask of 1024 bits. Generally the larger the key, the more difficult it is to guess.

Prior to encoding, the primary and convolution masks described above are generated by a cryptographically secure random generation process. It is possible to use a block cipher like DES in combination with a sufficiently pseudo-random seed value to emulate a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in decoding, should that step become necessary.

...

Starting with the lowest frequency band, the encoder proceeds through each band to the highest, visiting each of the 128 frequency bands in order. At each band value, the encoder takes the bit of the primary mask corresponding to the frequency band in question, the bit of the convolution mask corresponding to the window in question, and passes these values into a boolean function. This function is designed so that it has a near perfectly random output distribution. It will return true for approximately 50% of its input permutations, and false for the other 50%. The value returned for a given set of inputs is fixed, however, so that it will always return the same value given the same set of inputs.

If the function returns true, the current frequency band in the current window is used in the encoding process, and represents a valid piece of the additional information encoded in the signal. If the function returns false, this cell, as the frequency band in a given window is called, is ignored in the process. In this manner it is made extremely difficult to extract the encoded information from the signal without the use of the exact masks used in the encoding process. This is one place in which the stega-cipher process departs from traditional steganographic implementations, which offer a trivial decode opportunity if one knows the information is present. While this increases the information storage capacity of the carrier signal, it makes decoding trivial, and further degrades the signal. Note that it is possible and desirable to modify the boolean cell flag function so that it returns true <50% of the time. In general, the fewer cells actually used in the encode, the more difficult they will be to find and the less degradation of content will be caused, provided the function is designed correctly.

There is an obvious tradeoff in storage capacity for this increased security and quality.

The encoder proceeds in this manner until a complete copy of the additional information has been encoded in the carrier signal. It will be desirable to have the encoder encode multiple copies of the additional information continuously over the duration of the carrier signal, so that a complete instance of this information may be recovered from a smaller segment of a larger signal which has been split into discontinuous pieces or otherwise edited. It is therefore desirable to minimize the size of the information to be encoded using both compact design and pre-encoding compression, thus maximizing redundant encoding, and recoverability from smaller segments. In a practical implementation of this system it is

The encoder will also prepare the package of additional information so that it contains an easily recognizable start of message delimiter, which can be unique to each encoding and stored along with the keys, to serve as a synchronization signal to a decoder. The detection of this delimiter in a decoding window signifies that the decoder can be reasonably sure it is aligned to the sample stream correctly and can proceed in a methodic window by window manner. These delimiters will require a number of bits which minimizes the probability that this bit sequence is not reproduced in a random occurrence, causing an accidental misalignment of the decoder. A minimum of 256 bits is recommended. In the current implementation 1024 bits representing a start of message delimiter are used. If each sample is random, then each bit has a 50% probably of matching the delimiter and the conditional probability of a random match would be $1/2^{1024}$. In practice, the samples are probably somewhat less than random, increasing the probability of a match somewhat.

Specification, Page 26, lines13-18:

An average of 64 bits can be encoded into each window, which equals only 8 bytes. Messages larger than 8 bytes can be encoded by simply dividing the messages up and encoding small portions into a string of consecutive windows in the sample stream. Since the keys determine exactly how many bits will be encoded per window, and an element of randomness is desirable, as opposed to perfect predictability, one cannot be certain exactly how many bits are encoded into each window.

Initialization of Randomizer

Applicant confirms that the stega-cipher of the present invention uniquely marks each and every copy of data that is made using the invention. In other words, if you run the stega-cipher on the same carrier data, using the same message data, and the same random or pseudo random key, the output will be different each time the stega-cipher is run. (See Specification,

Page 9, lines 18-20, "The invention uniquely identifies every copy of multimedia content made using the invention...").

Powell

During the interview of December 4, 2001, the parties present discussed the published European application of Powell (0581317A2). Further to that discussion, Applicant submits that Powell does not disclose the use of a stega-cipher as claimed by the present invention for at least two reasons: 1) Powell does not disclose the use of a cipher; 2) Powell does not disclose the use of a key; and 3) Powell does not embed independent data into a carrier signal. In particular, Powell does not disclose the use of a cipher function that makes use of potential data location information, a random or pseudo random seed, and the message data to generate a key that maps the message data into the carrier signal. Powell does suggest that a computer "can be programmed to choose signature points randomly or accordingly to a predetermined pattern" (Powell, page. 4 lines, 40-42), but this is not the same as using a cipher to identify which extrema will be used. Moreover, Powell does not utilize any key—which is why the "image signature" can only be retrieved through the use of the original, unaltered image (Powell, page 5, line 51-page 6, line 9). The use of keys to encode also permits the use of keys to decode, resulting in a significant practical difference between Powell's teachings and those of the present invention. Since an object of the present invention is to protect the original data, it is undesirable (and, indeed, very risky) to circulate unwatermarked copies of the original data for decode purposes. Circulation of the decode key, rather than the original data, helps to protect the original data from the risk of unauthorized and untraceable copying.

Finally, Powell does not embed independent data into the digital image as required by the claimed invention. In Powell, the pixel value (which is a luminance value) is adjusted a small positive or negative amount (preferably 2% to 10% of the initial pixel value), whereby the difference is indicative of a "1" or a "0". (Powell, page 4 lines 42-48). Hence, Powell teaches replacing a pixel value with a new value that is dependent upon the initial value (adjusted upwards or downwards 2-10%) of the pixel. If the value was not dependent upon the initial value, the embedding would not be inconspicuous. Therefore, for at least this additional reason, Powell is distinguishable.

CONCLUSION

Applicant maintains that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representative, either by telephone or in person, would further prosecution of this application, we would welcome the opportunity for such an interview.

Respectfully submitted,

WILEY REIN & FIELDING L.L.P.

Dated: December 11, 2001

By: Floyd B Chapman
Floyd B. Chapman
Registration No. 40,555

Wiley Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006
202.719.7000 (Telephone)
202.719.7049 (Facsimile)